

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

JC525 U.S. PTO
09/557980



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

1999年 4月28日

出願番号
Application Number:

平成11年特許願第121200号

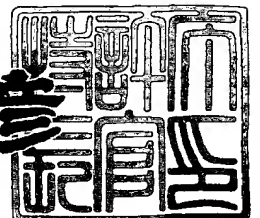
出願人
Applicant(s):

カシオ計算機株式会社

2000年 2月25日

特許庁長官
Commissioner,
Patent Office

近藤 隆彦



出証番号 出証特2000-3009972

【書類名】 特許願

【整理番号】 98-2289-00

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/00

【発明者】

【住所又は居所】 東京都羽村市栄町 3 丁目 2 番 1 号

カシオ計算機株式会社羽村技術センター内

【氏名】 森川 重則

【発明者】

【住所又は居所】 東京都羽村市栄町 3 丁目 2 番 1 号

カシオ計算機株式会社羽村技術センター内

【氏名】 井口 敏之

【発明者】

【住所又は居所】 東京都羽村市栄町 3 丁目 2 番 1 号

カシオ計算機株式会社羽村技術センター内

【氏名】 大塚 基

【特許出願人】

【識別番号】 000001443

【氏名又は名称】 カシオ計算機株式会社

【代理人】

【識別番号】 100074985

【弁理士】

【氏名又は名称】 杉村 次郎

【手数料の表示】

【予納台帳番号】 023180

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9109737

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ処理装置およびそのプログラム記録媒体

【特許請求の範囲】

【請求項 1】

アプリケーションソフト／データが格納されている持ち運び自在な記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスしてデータ処理を行うデータ処理装置において、

前記記録媒体内のアプリケーションソフト／データをアクセスする際に、データ処理装置固有の識別情報がアクセス制御情報としてその記録媒体内に予め格納されている場合に、この記録媒体から前記識別情報を読み込む読込手段と、

この読込手段によって読み込まれた識別情報と予め設定されている自己の識別情報とを比較する比較手段と、

この比較手段による比較結果に基づいて前記記録媒体内のアプリケーションソフト／データに対するアクセス可否を決定するアクセス制御手段とを具備したことを特徴とするデータ処理装置。

【請求項 2】

同一グループに属する複数台のデータ処理装置に対応してその装置固有の識別情報が複数格納されているグループ対応の記録媒体をアクセスする場合に、

前記アクセス制御手段は前記記録媒体から読み込んだ複数の識別情報の中に、予め設定されている自己の識別情報が含まれているか否かに基づいて当該記録媒体内のアプリケーションソフト／データに対するアクセス可否を決定するようにしたことを特徴とする請求項 1 記載のデータ処理装置。

【請求項 3】

前記記録媒体内に複数のアプリケーションソフト／データが格納されていると共に、個々のアプリケーションソフト／データに対応付けてデータ処理装置固有の識別情報が格納されている場合に、

前記読込手段はアクセス対象として指定されたアプリケーションソフト／データに対応する識別情報を読み込み、

前記アクセス制御手段は前記記録媒体から読み込まれた識別情報と予め設定さ

れている自己の識別情報とを比較することによりアプリケーションソフト／データ毎にアクセス可否を決定するようにしたことを特徴とする請求項 1 記載のデータ処理装置。

【請求項 4】

持ち運び自在な記録媒体にアプリケーションソフト／データを書き込むことにより、この記録媒体を介して各端末側にアプリケーションソフト／データを配布するデータ処理装置において、

アプリケーションソフト／データをアクセスすることが許可／禁止された端末に対して予め割り当てられている端末固有の識別情報をアクセス制御情報として取得する取得手段と、

この取得手段によって得られた端末識別情報をアプリケーションソフト／データに対応付けてその記録媒体内に書き込む書込手段とを具備したことを特徴とするデータ処理装置。

【請求項 5】

個々のアプリケーションソフト／データ毎にそのアクセスを許可／禁止する端末を定義する定義情報を参照し、前記書込手段は端末対応の記録媒体毎に書き込み対象としてのアプリケーションソフト／データを特定すると共に、特定されたアプリケーションソフト／データをその端末識別情報と共に記録媒体内に書き込むようにしたことを特徴とする請求項 4 記載のデータ処理装置。

【請求項 6】

同一グループに属する複数の端末へ前記記録媒体を介してアプリケーションソフト／データを配布する際に、前記取得手段は、そのグループに属する各端末固有の識別情報を複数取得し、

前記書込手段はこの取得手段によって得られた同一グループに属する複数の端末識別情報をアプリケーションソフト／データと共に書き込むようにしたことを特徴とする請求項 4 記載のデータ処理装置。

【請求項 7】

端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、

各アプリケーションソフト／データに対応して端末識別情報をアクセス制限情報として記憶するアクセス制限情報記憶手段と、

いずれかの端末装置からアプリケーションソフト／データに対するアクセス要求があった際に、要求元の端末装置から送信されて来た端末識別情報とアプリケーションソフト／データに対応する端末識別情報とを比較する比較手段と、

この比較手段による比較結果に基づいてアプリケーションソフト／データに対するアクセス可否を決定するアクセス制御手段とを具備したことを特徴とするデータ処理装置。

【請求項 8】

コンピュータによって読み取られるプログラムコードを有する記録媒体であって、

アプリケーションソフト／データが格納されている持ち運び自在な記録媒体がセットされている状態での記録媒体内のアプリケーションソフト／データをアクセスする際に、この記録媒体からデータ処理装置固有の識別情報を読み込む機能と、

この識別情報と予め設定されている自己の識別情報とを比較する機能と、

この比較結果に基づいて前記記録媒体内のアプリケーションソフト／データに対するアクセス可否を決定する機能を実現するためのプログラムコードを有する記録媒体。

【請求項 9】

コンピュータによって読み取られるプログラムコードを有する記録媒体であって、

アプリケーションソフト／データをアクセスすることが許可／禁止されている端末に対して予め割り当てられている端末固有の識別情報をアクセス制御情報として取得する機能と、

このアプリケーションソフト／データに対応付けてその記録媒体内に書き込む機能を実現するためのプログラムコードを有する記録媒体。

【請求項 10】

コンピュータによって読み取られるプログラムコードを有する記録媒体であって、

て、

いずれかの端末装置からネットワークを介してアプリケーションソフト／データに対するアクセス要求があった際に、要求元の端末装置から送信されて来た端末識別情報と、アプリケーションソフト／データに対応する端末識別情報とを比較する機能と、

この比較結果に応じてアプリケーションソフト／データに対するアクセス可否を決定する機能を実現するためのプログラムコードを有する記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、アプリケーションソフト／データのアクセスを制御するデータ処理装置およびそのプログラム記録媒体に関する。

【0002】

【従来の技術】

一般に、アプリケーションソフトはフロッピーディスクやコンパクトディスク等の記録媒体を介してパーソナルコンピュータ（パソコン）に別途提供され、これをパソコン上でインストールすることにより起動される。この場合、ソフトメーカーはアプリケーションソフトにユニークなプロダクト番号を付けて出荷する。このソフトをユーザがパソコン上でインストールして動作させる場合、許可キーとしてこのプロダクト番号をキーボードから入力するようにしている。

一方、複数台の端末装置がネットワークを介して通信接続されて成るオンライン型のクライアント・サーバシステムにおいて、各クライアント端末はネットワークを経由してアプリケーションソフトを入手するようにしている。この場合、クライアント端末からサーバへアプリケーションソフトのコピー転送を要求するが、その際、ユーザは自己のIDとパスワードを入力するようにしている。

【0003】

【発明が解決しようとする課題】

しかしながら、記憶媒体を介して提供されるアプリケーションソフトは、そのプロダクト番号さえ分かれば、複数台のパソコンに何回もインストールすること

ができ、不法なコピー複製が可能となる。このようなコピー複製を禁止するためには、一旦、アプリケーションソフトをインストールしたらその記憶媒体の内容を全てクリアする必要がある。しかしながら、記憶媒体の内容を全てクリアしてしまうと、その後、障害が発生し、再度インストールする必要が生じたときには、それに対応することができなくなり、また記憶媒体の内容をその都度クリアするという面倒な作業を強要することにもなる。

また、ネットワーク経由でクライアント端末からサーバへアクセスする場合、ユーザIDとパスワードとを知っていれば、誰でもどの端末からでもアプリケーションソフトをアクセスすることができ、不正アクセスの可能性がある。

このことはアプリケーションソフトに限らず、機密性の高い重要データを記憶媒体を介して提供する場合やネットワーク経由で提供する場合においても同様であり、セキュリティ維持の点で問題があった。

第1の発明の課題は、アプリケーションソフト／データが格納されている記録媒体をアクセスしてデータ処理を行うデータ処理装置において、特定のデータ処理装置に対してのみ記録媒体内のアプリケーションソフト／データのアクセスを許可することで、装置毎のアクセス制御が可能となり、セキュリティ維持と共にアクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止できるようにすることである。

第2の発明の課題は、アプリケーションソフト／データを記録媒体に書き込んで各端末に配布するデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可／禁止するための書き込みを行うことで、端末毎のアクセス制御が可能となりセキュリティ維持と共に、アクセス権限を有しない他の端末による不法なコピー複製を効果的に禁止できるようにすることである。

第3の発明の課題は、端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可することで、不法なアプリケーションソフト／データのダウンロードを禁止し、そのセキュリティを維持できるようにすることである。

【0004】

【課題を解決するための手段】

この発明の手段は次の通りである。

請求項 1 記載の発明（第 1 の発明）は、アプリケーションソフト／データが格納されている持ち運び自在な記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスしてデータ処理を行うデータ処理装置において、前記記録媒体内のアプリケーションソフト／データをアクセスする際に、データ処理装置固有の識別情報がアクセス制御情報としてその記録媒体内に予め格納されている場合に、この記録媒体から前記識別情報を読み込む読込手段と、この読込手段によって読み込まれた識別情報と予め設定されている自己の識別情報とを比較する比較手段と、この比較手段による比較結果に基づいて前記記録媒体内のアプリケーションソフト／データに対するアクセス可否を決定するアクセス制御手段とを具備するものである。

なお、同一グループに属する複数台のデータ処理装置に対応してその装置固有の識別情報が複数格納されているグループ対応の記録媒体をアクセスする場合に、前記アクセス制御手段は前記記録媒体から読み込んだ複数の識別情報の中に、予め設定されている自己の識別情報が含まれているか否かに基づいて当該記録媒体内のアプリケーションソフト／データに対するアクセス可否を決定するようにしてもよい。

また、前記記録媒体内に複数のアプリケーションソフト／データが格納されていると共に、個々のアプリケーションソフト／データに対応付けてデータ処理装置固有の識別情報が格納されている場合に、前記読込手段はアクセス対象として指定されたアプリケーションソフト／データに対応する識別情報を読み込み、前記アクセス制御手段は前記記録媒体から読み込まれた識別情報と予め設定されている自己の識別情報とを比較することによりアプリケーションソフト／データ毎にアクセス可否を決定するようにしてもよい。

請求項 1 記載の発明においては、アプリケーションソフト／データと共にデータ処理装置固有の識別情報（例えば、端末 ID）が格納されている記録媒体をアクセスする際に、この記録媒体から識別情報を読み込み、この識別情報と予め設定されている自己の識別情報とを比較し、この比較結果に基づいて記録媒体内の

アプリケーションソフト／データに対するアクセス可否を決定する。

したがって、アプリケーションソフト／データが格納されている記録媒体をアクセスしてデータ処理を行うデータ処理装置において、特定のデータ処理装置に対してのみ記録媒体内のアプリケーションソフト／データのアクセスを許可することで、装置毎のアクセス制御が可能となり、セキュリティ維持と共にアクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止することができる。

【 0 0 0 5 】

請求項 4 記載の発明（第 2 の発明）は、持ち運び自在な記録媒体にアプリケーションソフト／データを書き込むことにより、この記録媒体を介して各端末側にアプリケーションソフト／データを配布するデータ処理装置において、アプリケーションソフト／データをアクセスすることが許可／禁止された端末に対して予め割り当てられている端末固有の識別情報をアクセス制御情報として取得する取得手段と、この取得手段によって得られた端末識別情報をアプリケーションソフト／データに対応付けてその記録媒体内に書き込む書込手段とを具備するものである。

なお、個々のアプリケーションソフト／データ毎にそのアクセスを許可／禁止する端末を定義する定義情報を参照し、前記書込手段は端末対応の記録媒体毎に書き込み対象としてのアプリケーションソフト／データを特定すると共に、特定されたアプリケーションソフト／データをその端末識別情報と共に記録媒体内に書き込むようにしてもよい。

また、同一グループに属する複数の端末へ前記記録媒体を介してアプリケーションソフト／データを配布する際に、前記取得手段は、そのグループに属する各端末固有の識別情報を複数取得し、前記書込手段はこの取得手段によって得られた同一グループに属する複数の端末識別情報をアプリケーションソフト／データと共に書き込むようにしてもよい。

請求項 4 記載の発明においては、アプリケーションソフト／データをアクセスすることが許可／禁止された端末に対して予め割り当てられている端末固有の識別情報を取得し、この識別情報をアプリケーションソフト／データに対応付けて

その記録媒体内に書き込む。

したがって、アプリケーションソフト／データを記録媒体に書き込んで各端末に配布するデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可／禁止するための書き込みを行うことで、端末毎のアクセス制御が可能となりセキュリティ維持と共に、アクセス権限を有しない他の端末による不法なコピー複製を効果的に禁止することができる。

【0006】

請求項7記載の発明（第3の発明）は端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、各アプリケーションソフト／データに対応して端末識別情報をアクセス制限情報として記憶するアクセス制限情報記憶手段と、いずれかの端末装置からアプリケーションソフト／データに対するアクセス要求があった際に、要求元の端末装置から送信されて来た端末識別情報とアプリケーションソフト／データに対応する端末識別情報とを比較する比較手段と、この比較手段による比較結果に基づいてアプリケーションソフト／データに対するアクセス可否を決定するアクセス制御手段とを具備するものである。

請求項7記載の発明においては、いずれかの端末装置からアプリケーションソフト／データに対するアクセス要求があった際に、要求元の端末装置から送信されて来る端末識別情報と、アプリケーションソフト／データに対応する端末識別情報とを比較し、その比較結果に応じてアプリケーションソフト／データに対するアクセス可否を決定する。

したがって、端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可することで、不法なアプリケーションソフト／データのダウンロードを禁止し、そのセキュリティを維持することができる。

【0007】

【発明の実施の形態】

（第1実施形態）

以下、図1～図7を参照してこの発明の第1実施形態を説明する。

図1はオフライン型のクライアント・サーバシステムを示したシステム構成図

である。すなわち、会社組織において、会社内に設置されているサーバコンピュータ 1 と、各営業担当者が持参するモバイル型のクライアント端末（携帯端末） 2 とを有し、各営業担当者は外出先で可搬型記録媒体 3 内のアプリケーションソフト／データベースをアクセスしながら営業活動を行い、そして、一日の営業終了時に、端末本体から可搬型記録媒体 3 を抜き取り、サーバコンピュータ 1 のカードリーダー／ライタ 4 にセットすると、サーバコンピュータ 1 はカードリーダー／ライタ 4 を介して CF カード 3 内の営業記録を収集処理するオフライン型のシステムである。ここで、可搬型の記録媒体 3 は取り外し可能なコンパクトフラッシュカードであり、以下、CF カード 3 と称する。サーバコンピュータ 1 に付属されているカードリーダー／ライタ 4 は、各クライアント端末対応の CF カード 3 が複数枚同時にセット可能なもので、各 CF カード 3 を順次アクセスしてデータの読み込み／書き込みを行う。なお、図中、CF カード 3 に付した「# 1」、「# 2」、「# 3」は、端末名称 {A 1}、「B 1」、「C 1」で示される携帯端末 2 に対応付けられ、携帯端末 2 と 1 : 1 に対応付けられた端末対応の CF カード 3 であることを示している。なお、この実施形態においては端末対応の CF カード 3 の他、後述する端末グループ対応の CF カード 3 も存在するが、図 1 の例では端末対応の CF カード 3 のみを示している。サーバコンピュータ 1 はこの CF カード 3 を介して携帯端末 2 側へアプリケーションソフト（AP ソフト）／データベースを配布する。すなわち、サーバコンピュータ 1 は AP ソフト格納部 5、データベース格納部 6 の内容を読み出してカードリーダー／ライタ 4 に与え、それにセットされている各 CF カード 3 に AP ソフト／データベースを書き込むが、その際、サーバコンピュータ 1 は端末登録テーブル 7、アプリ・データ設定テーブル 8 を参照してどの端末に何を書き込むかを判別し、AP ソフト／データベースを特定して該当する CF カード 3 内に書き込むと共に端末識別情報（端末 ID）を AP ソフト／データベースに対するアクセス制御情報として CF カード 3 内に書き込む。

【0008】

図 2 は CF カード 3 に格納されているデータを示したもので、（A）は端末対応の CF カード 3 の内容を示している。この端末対応の CF カード 3 は、それを

識別するための固有の媒体番号と、このカードを専用する携帯端末 2 を識別するための固有の端末 ID と、AP ソフト、データベースとを記憶する構成で、この例では媒体番号「M 0 1」、端末 ID「ID 1 1」、AP ソフト「α 1」、データベース「D 1」が格納されている。ここで、AP ソフト／データベースと端末 ID との対応関係は、そのアクセスを許可する端末を定義するもので、端末対応の CF カード 3 には 1 種類の端末 ID が設定されている。

また、図 2 (B) は端末グループ A 対応の CF カード 3 の内容を示し、図 3 に示すように「# 1 A」を付した各 CF カード 3 は、端末名称が「A 1」、「A 2」、「A 3」である各携帯端末 2 が属する端末グループ A 対応の記憶媒体で、そのグループ対応の各 CF カード 3 には、「媒体番号」の他、各種の AP ソフト／データベース毎に 1 または 2 以上の端末 ID が格納されており、「媒体番号」を除く他のデータは、そのグループ内において同一内容となっている。なお、図 2 (A) で示した端末 ID は図 3 に示すように端末グループ A に属する各携帯端末 2 毎に割り当てられた固有の端末識別情報であり、AP ソフト／データベースと端末 ID との対応関係は、端末対応の場合と同様に、そのアクセスを許可する端末を定義する。また、図 2 (C) は端末グループ B 対応の CF カード 3 の内容を示し、そのデータ構造は図 2 (B) で示した端末グループ A の場合と同様であるため、その説明は省略するが、端末グループ B 対応の各 CF カード 3 内に設定された端末 ID は、図 3 に示すように端末グループ B に属する各携帯端末 2 毎に割り当てられた端末識別情報である。

【0 0 0 9】

図 4 はサーバコンピュータ 1 側に設けられている端末登録テーブル 7、アプリ・データ設定テーブル 8、グループ登録テーブル 9 のデータ構造を示したもので、図 4 (A) は端末登録テーブル 7 の内容を示している。この端末登録テーブル 7 はアプリ・データ設定テーブル 8 を作成する際や端末対応の CF カード 3 に AP ソフト／データベースを書き込む際に参照されるもので、「端末名称」、「端末 ID」、「媒体番号」とを対応付けた構成で、システム構築時や新たな媒体を追加採用するとき等にその設定登録が行われる。アプリ・データ設定テーブル 8 は図 4 (B) に示すように、AP ソフト／データベース毎に、そのソフト名／デ

ータベース名に対応付けて、1または2以上の端末IDを記憶する構成で、サーバコンピュータ1はCFカード3にAPソフト／データベースを書き込む際に参照される。

【0010】

図5は、サーバコンピュータ1、携帯端末2の全体構成を示したブロック図である。なお、サーバコンピュータ1、携帯端末2の構成要素は基本的に同一であるため、図中11～16はサーバコンピュータ1に対応する構成要素とし、図中21～26は携帯端末2に対応する構成要素として以下、説明するものとする。

CPU11(21)は各種プログラムにしたがってこのサーバコンピュータ1(携帯端末2)の全体動作を制御する中央演算処理装置である。記憶装置12(22)はオペレーティングシステムや各種アプリケーションプログラム、データベース、文字フォントデータ等が予め格納されている記憶媒体13(23)やその駆動系を有している。この記憶媒体13(23)は固定的に設けたもの、もしくは着脱自在に装着可能なものであり、フロッピーディスク、ハードディスク、光ディスク、RAMカード等の磁氣的・光学的記憶媒体、半導体メモリによって構成されている。また、記憶媒体内のプログラムやデータは、必要に応じてCPU11(21)の制御により、RAM14(24)にロードされる。更に、CPU11(21)は通信回線等を介して他の機器側から送信されて来たプログラム、データを受信して記憶媒体に格納したり、他の機器側に設けられている記憶媒体に格納されているプログラム、データを通信回線等を介して使用することもできる。また、CPU11(21)にはその入出力周辺デバイスである入力装置15(25)、表示装置16(26)がバスラインを介して接続されており、入出力プログラムにしたがってCPU11(21)はそれらの動作を制御する。

【0011】

次に、このクライアント・サーバシステムの動作を図6および図7に示すフローチャートにしたがって説明する。ここで、これらのフローチャートに記述されている各機能を実現するためのプログラムは、読み取り可能なプログラムコードの形態で記憶媒体13(23)に格納されており、CPU11(21)はこのプログラムコードにしたがった動作を逐次実行する。なお、このことは後述する他

の実施形態についても同様である。

図 6 はサーバコンピュータ 1 側の特徴的な動作を示したフローチャートである。

。 先ず、アプリ・データ設定テーブル 8 に対してその内容を任意に設定する設定登録が指示された場合には（ステップ A 1）、アプリ・データ設定テーブル 8 に設定すべき AP ソフト／データベースの名称を選択すると共に、この AP ソフト／データベースに対してそのアクセスを許可する携帯端末 2 の端末名称を選択する（ステップ A 3）。すると、選択された AP ソフト／データベースの名称がアプリ・データ設定テーブル 8 に書き込まれるときに、選択された端末名称に対応する端末 ID を端末登録テーブル 7 から取得し、この端末 ID を AP ソフト／データベースの名称に対応付けてアプリ・データ設定テーブル 8 に書き込む（ステップ A 4）。このようにして 1 レコード分のデータをアプリ・データ設定テーブル 8 に設定し終ると、設定終了が指示されたかを調べ（ステップ A 5）、設定終了が指示されるまで上述の動作が繰り返される（ステップ A 2 ～ A 4）。

【 0 0 1 2 】

次に、CF カード 3 への書き込みが指示された場合には（ステップ A 6）、カードリーダー／ライタ 4 に CF カード 3 がセットされていることを条件に（ステップ A 7）、CF カード 3 への書き込み処理に移る。先ず、書き込みタイプの選択を行う（ステップ A 8）。ここで、ユーザは端末対応の CF カード 3 への書き込みか、端末グループ対応の CF カード 3 への書き込みかを選択指定すると、選択された書き込み形式の判別が行われる。いま、端末対応の書き込みが選択指定された場合には、カードリーダー／ライタ 4 にセットされている CF カード 3 から「媒体番号」を読み出し（ステップ A 9）、媒体番号対応の端末 ID を端末登録テーブル 7 から取得する（ステップ A 10）。そして、端末 ID に基づいてアプリ・データ設定テーブル 8 を検索し、端末 ID 対応の AP ソフト／データベースの名称を取得し、それに応じて AP ソフト格納部 5、データベース格納部 6 から該当する AP ソフト／データベースを読み出す（ステップ A 11）。いま、図 4（B）に示すアプリ・データ設定テーブル 8 において、端末 ID が「ID 1 1」であれば、それに該当する AP ソフトとして「α 1」、データベースとして「D 1

」がAPソフト格納部5、データベース格納部6から読み出される。

【0013】

このようにして取得した端末ID対応のAPソフト／データベースをそのCFカード3へ書き込むと共に（ステップA12）、上述のステップA10で取得した端末IDをそのAPソフト／データベースに対するアクセス制御情報として書き込む（ステップA13）。このような書き込みが終ると、その端末IDに対応してアプリ・データ設定テーブル8に書き込み済であることを示す「書き込みフラグ」をセットする（ステップA14）。そして、カードリーダー／ライター4に複数枚のCFカード3がセットされてる場合、未書き込みのCFカード3が有るかを調べ（ステップA15）、有ればステップA9に戻り、次のCFカード3をアクセスしてその「媒体番号」を読み出し、そのCFカード3に対して上述と同様の書き込み処理を行う。これによってセット中の全てのCFカード3に対してその書き込みが終ると、アプリ・データ設定テーブル8を参照し、「書き込みフラグ」がセットされていない端末IDを抽出し、この端末IDに該当する端末名称を端末登録テーブル7から取得し、未書き込み端末名称として一覧表示させると共に（ステップA16）、書き込み完了メッセージを表示出力させる（ステップA17）。

【0014】

一方、端末グループ対応のCFカード3に対応する書き込みが選択指定された場合には、端末グループ名の選択画面が表示され、その中から所望のグループ名を選択指定すると（ステップA18）、このグループ名に基づいてグループ登録テーブル9を検索し、該当する複数の端末IDを取得する（ステップA19）。そして、この複数の端末IDに基づいてアプリ・データ設定テーブル8の内容をその先頭から検索し、その端末IDが1つでも含まれていれば、それに対応するAPソフト／データベースをAPソフト格納部5、データベース格納部6から読み出す（ステップA20）。ここで、端末グループAが選択された場合には、APソフト「α1」を取得する。そして、取得したAPソフト／データベースをそれに対応する端末IDと共にCFカード3に書き込む（ステップA21、A22）。この場合、APソフト「α1」と端末ID「ID11」、「ID12」とが

対応付けられてCFカード3に書き込まれる。そして、カードリーダー/ライター4にセットされている全てのCFカード3に対して同様の書き込みが終了するまで柔術の動作が繰り返される（ステップA21～A23）。これによって全媒体への書き込みが終ると、ステップA24に進み、同一グループ内において未書き込みのAPソフト/データベースがアプリ・データ設定テーブル8内にまだ有るかを調べ、有ればステップA20に戻るため、次に、端末グループAに該当するAPソフトとして「α2」が読み出され、端末ID「ID13」と共に各CFカード3に書き込まれる。以下、同様に、データベース「D1」、端末ID「ID11」が各CFカード3に書き込まれ、次でデータベース「D2」、端末ID「ID12」、更にデータベース「D3」、端末ID「ID13」が各CFカード3に書き込まれる。この結果、端末グループA対応の各CFカード3の内容は、図2（B）に示す如くとなり、端末グループA対応の書き込みが全て完了すると、書き込み完了メッセージが表示される（ステップA17）。このようにしてAPソフト/データベースの書き込みが行われたCFカード3は、対応する携帯端末2側へそれぞれ配布される。

【0015】

図7は携帯端末2側の動作を示したフローチャートであり、電源投入に伴って実行開始される。先ず、初期メニュー画面の中から任意のAPソフト/データベースが選択されてその起動アクセスが指示された場合に（ステップB1）、その携帯端末2にCFカード3がセットされていなければ（ステップB2）、その起動アクセスを無効とするためにステップB1に戻るが、CFカード3がセットされていれば、予め設定されている自己の端末IDを読み出す（ステップB3）。そして、CFカード3をアクセスしてそれに格納されている端末IDを読み出し（ステップB4）、自己の端末IDと一致するかを調べる（ステップB5）。この場合、グループ対応のCFカード3にはAPソフト/データベース毎にそのグループに属する他の端末IDも格納されているので、選択指定されたAPソフト/データベースに対応する端末IDをCFカード3から読み出し、その中に自己の端末IDが含まれているかを調べる。ここで、端末IDの一致が検出された場合にはそれを条件に選択指定されたAPソフト/データベースのアクセスが許可

され、それに応じた処理の実行に移行するが（ステップB6）、端末IDの不一致が検出された場合にはステップB1に戻るため、そのAPソフト／データベースのアクセスは禁止される。

【0016】

以上のようにこの第1実施形態において、CFカード3内のAPソフト／データベースをアクセスしてデータ処理を行う際に、携帯端末2はCFカード3から読み込んだ端末IDと予め設定されている自己の端末IDとを比較し、その一致／不一致によってCFカード3内のAPソフト／データベースに対するアクセスが制御されるので、特定の携帯端末2に対してのみCFカード3内のAPソフト／データベースをアクセスすることが可能となる。つまり、CFカード3内のAPソフト／データベースをアクセスすることができる携帯端末2を制限するようにしたから、端末毎のアクセス制御が可能となると共に、アクセス権限を有しない他の携帯端末2による不法なコピー複製を効果的に禁止することができる。

このことは端末対応のCFカード3に限らず、グループ対応のCFカード3についても同様であり、営業地域毎に特定のAPソフト／データベースを使用する場合、地域毎に端末グループを分けておけば、端末グループ毎のアクセス制御が可能となる。またCFカード3内に個々のAPソフト／データベースに対応付けて端末IDが格納されている場合には、端末毎、APソフト／データベース毎にそのアクセス制御が可能となる。すなわち、CFカード3内に複数のAPソフト／データベースが格納されている場合、特定のAPソフト／データベースに対してはアクセスが許可されるが、他のAPソフト／データベースについてはそのアクセスを禁止することができ、同一の端末グループに属する携帯端末2であっても、APソフト／データベース毎にそのアクセスを制御することが可能となる。

【0017】

一方、サーバコンピュータ1はCFカード3内のAPソフト／データベースを書き込むことによりこのCFカード3を介して携帯端末2側にAPソフト／データベースを配布するが、その際、サーバコンピュータ1はこのCFカード3に対応付けられている端末IDを読み出してCFカード3内にAPソフト／データベースと共にこの端末IDを書き込むようにしたから、APソフト／データベース

のアクセスを許可する携帯端末 2 を特定することができる。これによって端末毎のアクセス制御が可能となると共に、アクセス権限を有しない他の携帯端末 2 による不法なコピー複製を効果的に禁止することができる。また、サーバコンピュータ 1 は個々の AP ソフト／データベース毎にそのアクセスを許可する端末を定義するアプリ・データ設定テーブル 8 を参照することによって端末対応の CF カード 3 毎に、書き込み対象の AP ソフト／データベースを特定することができる。

このことは、端末対応の CF カード 3 に限らず、グループ対応の CF カード 3 についても同様であり、同じ端末グループに属する各携帯端末 2 の端末 ID を CF カード 3 内に書き込むことで、AP ソフト／データベースのアクセスを許可する端末グループを特定することができ、これによって端末グループ毎のアクセス制御が可能となる。

【0018】

なお、上述した第 1 実施形態は持ち運び自在な記憶媒体として CF カードを示したが、これに限らず、磁氣的、光学的記録媒体、半導体メモリ等、任意であり、またカード型に限らず、カートリッジ型のディスク等であってもよい。また、クライアント端末はモバイル型の携帯端末 2 に限らず、デスクトップ型の端末であってもよい。更に、記録媒体内の AP ソフト／データベースに対応してそのアクセスを許可する端末 ID を書き込む場合に限らず、そのアクセスを禁止する端末 ID を書き込むようにしてもよい。

【0019】

(第 2 実施形態)

以下、図 8～図 10 を参照してこの発明の第 2 実施形態を説明する。なお、上述した第 1 実施形態においては、持ち運び自由な可搬型の記憶媒体を介してサーバコンピュータ 1 と携帯端末 2 との間でデータの授受を行うオフライン型のクライアント・サーバシステムを示したが、この第 2 実施形態は複数台のクライアント端末がネットワークを介してサーバコンピュータに通信接続されて成るオンライン型のクライアント・サーバシステムに適用したもので、基本的には第 1 実施形態と同様の構成となっている。

【 0 0 2 0 】

図 8 はこの第 2 実施形態におけるクライアント・サーバシステムを示したシステム構成図であり、このクライアント・サーバシステムはサーバコンピュータ 3 1 に専用回線あるいは公衆回線を介して複数台のクライアント端末 3 2 が接続されたローカルエリアネットワークあるいは広域ネットワークシステムである。このサーバコンピュータ 3 1 側には端末登録テーブル 3 3、アプリ・データ設定テーブル 3 4 が設けられている。この端末登録テーブル 3 3、アプリ・データ設定テーブル 3 4 は上述した第 1 実施形態で示した端末登録テーブル 7、アプリ・データ設定テーブル 8（図 4（A）、（B）参照）と基本的に同様の構成で、端末登録テーブル 3 3 は「端末名称」、「端末 ID」とを対応付けた構成となっている。また、アプリ・データ設定テーブル 3 4 は AP ソフト／データベース毎にそのアクセスを許可する端末を識別するための端末 ID を対応付けて記憶するもので、各 AP ソフト／データベースに対応付けて 1 または 2 以上の端末 ID が記憶されている。ここで、クライアント端末 3 2 側から AP ソフト／データベースの送信要求が有った際に、サーバコンピュータ 3 1 は端末登録テーブル 3 3、アプリ・データ設定テーブル 3 4 を参照し、要求された AP ソフト／データベースに対してそのアクセスが許可されている端末からの要求であれば、それを条件に、AP ソフト／データベースを要求元へ送信するようにしている。

【 0 0 2 1 】

次に、この第 2 実施形態の動作を図 9、図 1 0 に示すフローチャートにしたがって説明する。図 9 はクライアント端末 3 2 側の動作を示し、図 1 0 はサーバコンピュータ 3 1 側の動作を示したフローチャートである。

先ず、クライアント端末 3 2 側において、自己の端末 ID をサーバコンピュータ 3 1 側の端末登録テーブル 3 3 に登録すべき ID 登録が指示された場合には（ステップ C 1）、自己の端末名称を入力したのち（ステップ C 2）、予め設定されている自己の端末 ID を読み出し（ステップ C 3）、サーバコンピュータ 3 1 に対して ID 登録を要求し、OK 応答（肯定応答）が有るまで ID 登録を要求し続ける（ステップ C 4、C 5）。ここで、OK 応答が有れば、端末 ID をサーバコンピュータ 3 1 へ送信する（ステップ C 6）ここで、サーバコンピュータ 3 1

側においては、端末側からの要求がID登録であれば（ステップD2～D4）、その要求を正常に受信したことを示すために要求元へOK応答を返信し（ステップD16）、これによってクライアント端末32側から送信されて来る端末名称、端末IDを受信すると（ステップD17）、それが予め決められている書式通りのデータであれば（ステップD18）、端末登録テーブル33にこの端末名称と端末IDとを対応付けて登録する（ステップD19）。そして、正常登録した旨を示すために、要求元へOK応答を行う（ステップD20）。一方、端末から送信されて来た端末名称、端末IDが書式通りのデータでなければ、要求元に対してエラー応答を行う（ステップD15）。これによってクライアント端末32側ではサーバコンピュータ31からの応答がOK応答であれば（ステップC7）、登録終了メッセージを表示させるが（ステップC8）、エラー応答であればエラーメッセージを表示させる（ステップC9）。

【0022】

このようにサーバコンピュータ31は各クライアント端末32からID登録が要求される毎に、端末名称、端末IDとを対応付けて端末登録テーブル33に順次登録してゆく。一方、サーバコンピュータ31側において、APソフト／データベースに対するアクセスをどの端末に許可するかをAPソフト／データベース毎に設定するために、その設定を指示すると、上述した第1実施形態と同様の処理（図6のステップA1～A5）によってアプリ・データ設定テーブル34が作成される（ステップD1、D5～D8）。このようにサーバコンピュータ31側に端末登録テーブル33、アプリ・データ設定テーブル34が作成されている状態で、クライアント端末32側でAPソフト／データベースの送信要求を指示すると（図10のステップC10）、予め設定されている自己の端末IDを読み出し（ステップC11）、サーバコンピュータ31に対してAPソフト／データベースの送信要求を行いOK応答が有るまで要求し続け（ステップC12、C13）、OK応答が有れば端末IDを送信する（ステップC14）。

【0023】

一方、サーバコンピュータ31側においては、クライアント端末32からの要求がAPソフト／データベースの送信要求であれば（ステップD2、D3）、要

求元へOK応答を送信したのち（ステップD9）、端末IDの受信待ちとなり、要求元からの端末IDを受信すると（ステップD10）、受信した端末IDに基づいて端末登録テーブル33を検索し、予め登録されている正規の端末からの要求であるかを調べる（ステップD11）。ここで、正規の端末からの要求でなければ、その要求元へエラー応答を行うが（ステップD15）、正規の端末からの要求であれば、要求元へOK応答を行うと共に（ステップD12）、その端末IDに基づいてアプリ・データ設定テーブル34を検索し、端末ID対応のAPソフト／データベースを選択的に読み出して要求元へ送信する（ステップD13、D14）。この場合、端末ID対応のAPソフト／データベースが複数存在していれば、その全てを要求元へ送信するようにしてもよいが、所望のAPソフト／データベースのみの送信要求があれば、要求されたAPソフト／データベースだけを送信する。

すると、クライアント端末32側においては、サーバコンピュータ31からエラー応答が有れば（ステップC15）、エラーメッセージを表示出力させるが（ステップC9）、OK応答が有れば（ステップC15）、サーバコンピュータ31側から通信されて来たAPソフト／データベースを受信して登録保存する（ステップC16、C17）。そして、このAPソフト／データベースを起動させてデータ処理を開始する（ステップC18）。なお、サーバコンピュータ31からのAPソフト／データベースが登録保存されている状態においては、その起動指示に応じていつでも自由にAPソフト／データベースにしたがったデータ処理を実行することができる（ステップC19、C18）。

【0024】

以上のようにこの第2実施形態におけるオンライン型のクライアント・サーバシステムにおいては、いずれかのクライアント端末32からAPソフト／データベースに対するアクセス要求があった際に、要求元のクライアント端末32から送信されて来た端末IDと、アプリ・データ設定テーブル34内のAPソフト／データベースに対応する端末IDとを比較し、その比較結果に応じてAPソフト／データベースに対するアクセス可否を決定するようにしたから、特定端末に対してのみAPソフト／データベースのアクセスを許可することで、不法なAPソ

フト／データベースのダウンロードを禁止し、そのセキュリティを維持することが可能となる。

【0025】

なお、上述した第2実施形態においては、端末登録テーブル33を設けたが、アプリ・データ設定テーブル34だけ設ける構成としてもよい。また、APソフト／データベースの送信要求に応じてAPソフト／データベースを要求元へ送信するようにしたが、クライアント端末32がサーバコンピュータ31内のAPソフト／データベースを直接アクセスするようにしてもよい。またオンライン型システムに限らず、無線通信や光通信を媒体とするシステムであってもよい。

また、上述した各実施形態において、端末IDの構成は任意であり、端末製造時の製造番号、例えば、「国コード＋製造会社コード＋機能コード＋端末シリアル番号」であってもよい。また公衆電話回線をネットワークとするシステムにおいては、「国電話コード＋地域電話コード＋電話番号」であってもよい。

更に、APソフト／データベースと端末IDとを対応付けたテーブルに限らず、APソフト／データベース毎にそのアクセスを許可する端末あるいはそのアクセスを禁止する端末を論理条件式で記述したテーブルとしてもよい。例えば、等号、不等号を用いて端末IDの番号が所定範囲内にあればアクセス可あるいは不可を定義するようにしてもよい。

【0026】

【発明の効果】

第1の発明によれば、アプリケーションソフト／データが格納されている記録媒体をアクセスしてデータ処理を行うデータ処理装置において、特定のデータ処理装置に対してのみ記録媒体内のアプリケーションソフト／データのアクセスを許可することで、装置毎のアクセス制御が可能となり、セキュリティ維持と共にアクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止することができる。

第2の発明によれば、アプリケーションソフト／データを記録媒体に書き込んで各端末に配布するデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可／禁止するための書き込みを行うことで

、端末毎のアクセス制御が可能となりセキュリティ維持と共に、アクセス権限を有しない他の端末による不法なコピー複製を効果的に禁止することができる。

第3の発明は、端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可することで、不法なアプリケーションソフト／データのダウンロードを禁止し、そのセキュリティを維持することができる。

【図面の簡単な説明】

【図1】

オフライン型のクライアント・サーバシステムを示したシステム構成図。

【図2】

(A) 端末対応のCFカード3内のデータを示した図、(B)は端末グループA対応のCFカード3内のデータを示した図、(C)は端末グループB対応のCFカード3内のデータを示した図。

【図3】

端末グループA、端末グループBを説明するための図。

【図4】

(A)は端末登録テーブル7のデータ構造を示した図、(B)はアプリ・データ設定テーブル8のデータ構造を示した図、(C)はグループ登録テーブル9のデータ構造を示した図。

【図5】

サーバコンピュータ1（携帯端末2）の全体構成を示したブロック図。

【図6】

サーバコンピュータ1側の特徴的な動作を示したフローチャート。

【図7】

携帯端末2側の特徴的な動作を示したフローチャート。

【図8】

第2実施形態におけるオンライン型クライアント・サーバシステムを示したシステム構成図。

【図9】

第 2 実施形態においてクライアント端末 3 2 側の動作を示したフローチャート

。

【図 1 0】

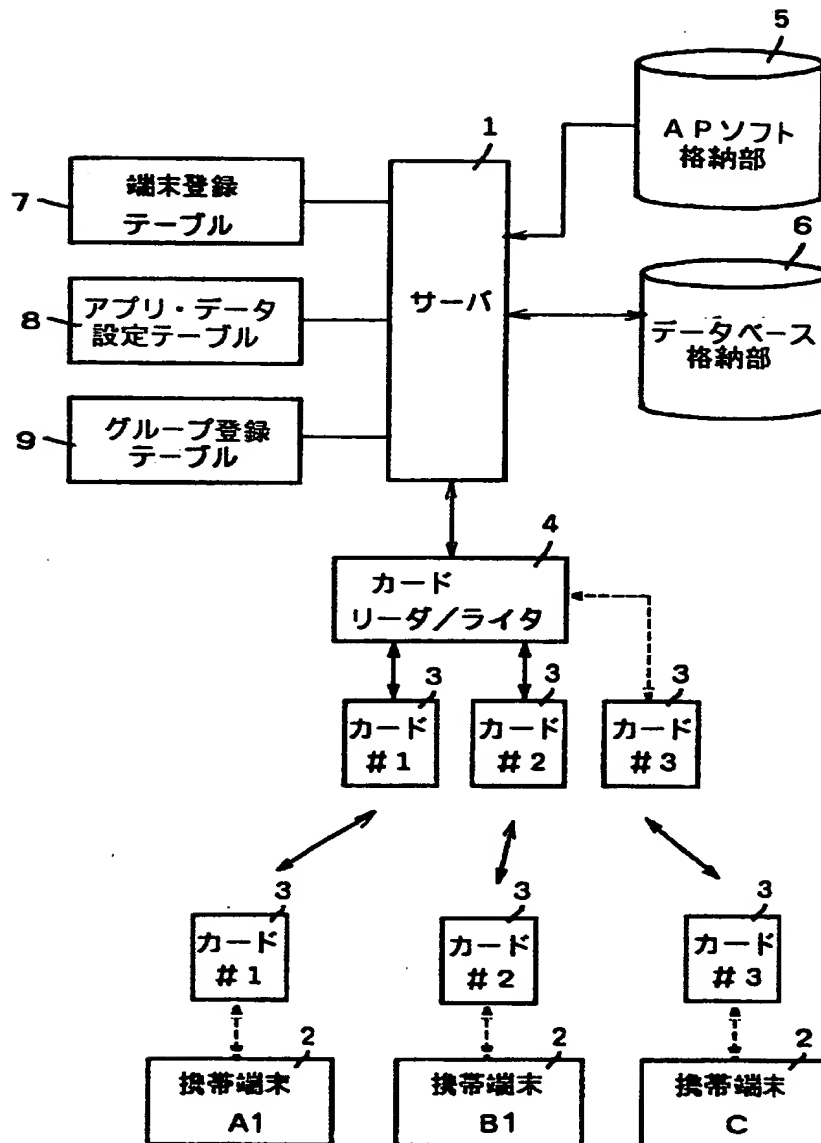
第 2 実施形態においてサーバコンピュータ 3 1 側の動作を示したフローチャート。

【符号の説明】

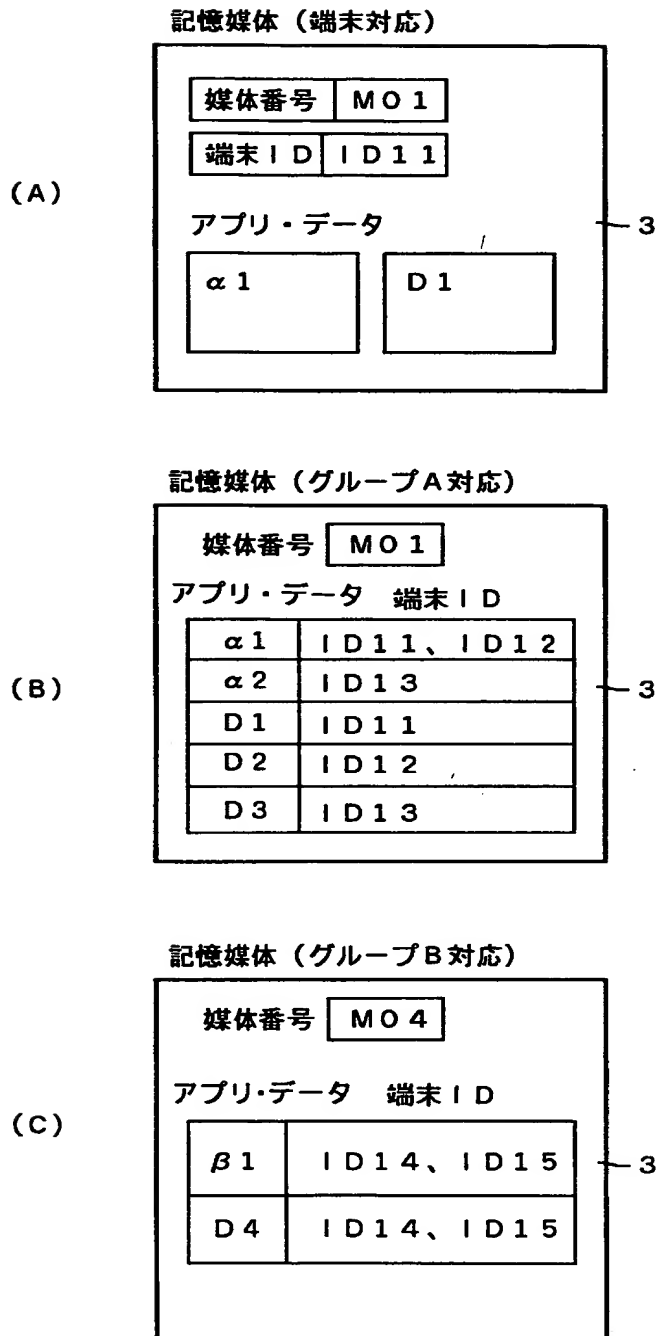
- 1、 3 1 サーバコンピュータ
- 2 携帯端末
- 3 C F カード
- 4 カードリーダー／ライター
- 5 A P ソフト格納部
- 6 データベース格納部
- 7、 3 3 端末登録テーブル
- 8、 3 4 アプリ・データ設定テーブル
- 9 グループ登録テーブル
- 3 2 クライアント端末
- A、 B 端末グループ

【書類名】 図面

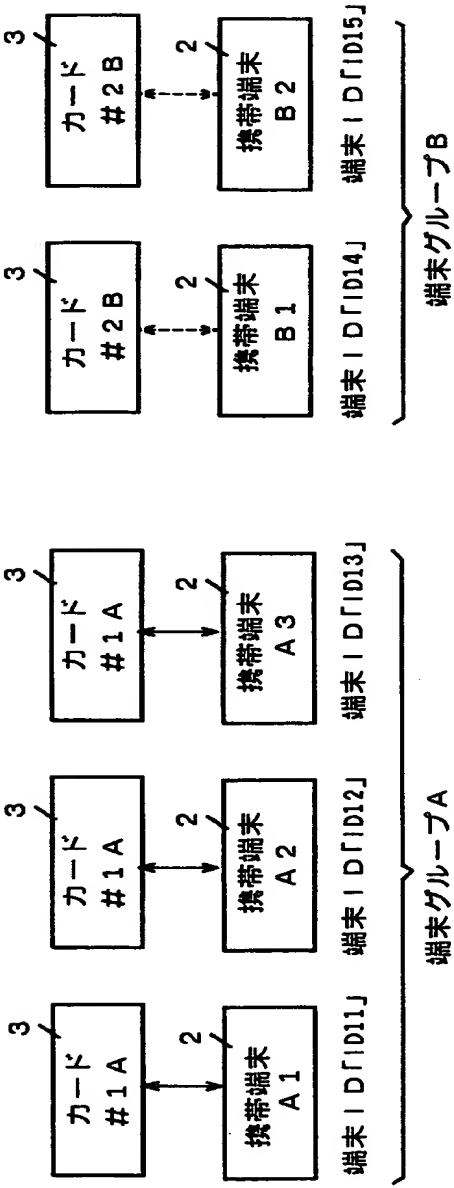
【図 1】



【図 2】



【図 3】



【図 4】

端末登録テーブル

(A)

端末名称	端末ID	媒体番号
A 1	ID 1 1	M 0 1
A 2	ID 1 2	M 0 2
A 3	ID 1 3	M 0 3
B 1	ID 1 4	M 0 4
B 2	ID 1 5	M 0 5

7

アプリ、データ設定テーブル

(B)

アプリデータ	端末ID	書き込みフラグ
アプリα 1	ID 1 1	
	ID 1 2	
アプリα 1	ID 1 3	
アプリβ 1	ID 1 5	
	ID 1 4	
データD 1	ID 1 1	
データD 2	ID 1 2	
データD 3	ID 1 3	
データD 4	ID 1 4	
	ID 1 5	

8

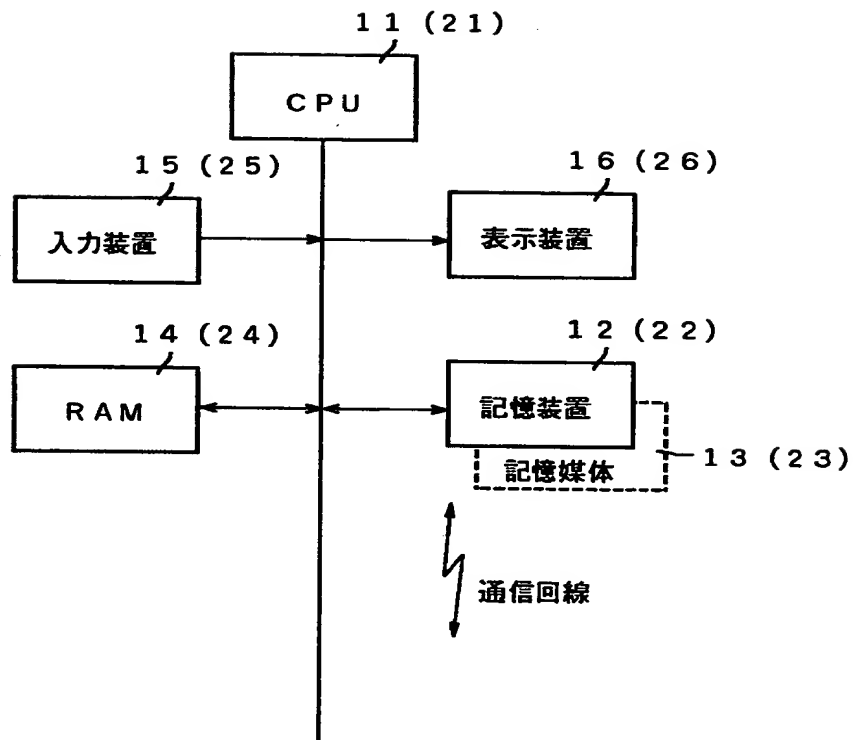
グループ登録テーブル

(C)

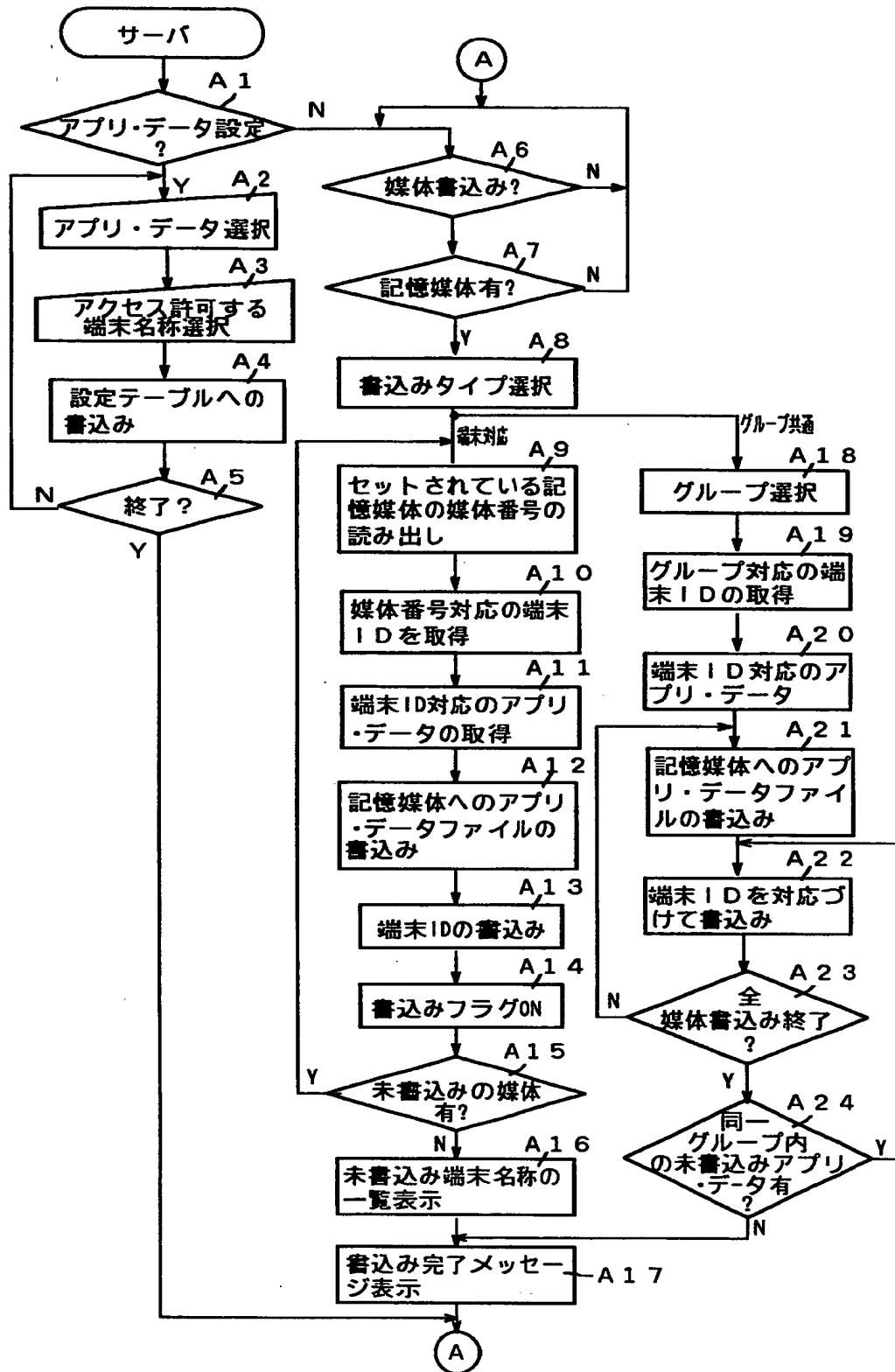
端末グループ名称	端末ID
A	ID 1 1
	ID 1 2
	ID 1 3
B	ID 1 4
	ID 1 5

9

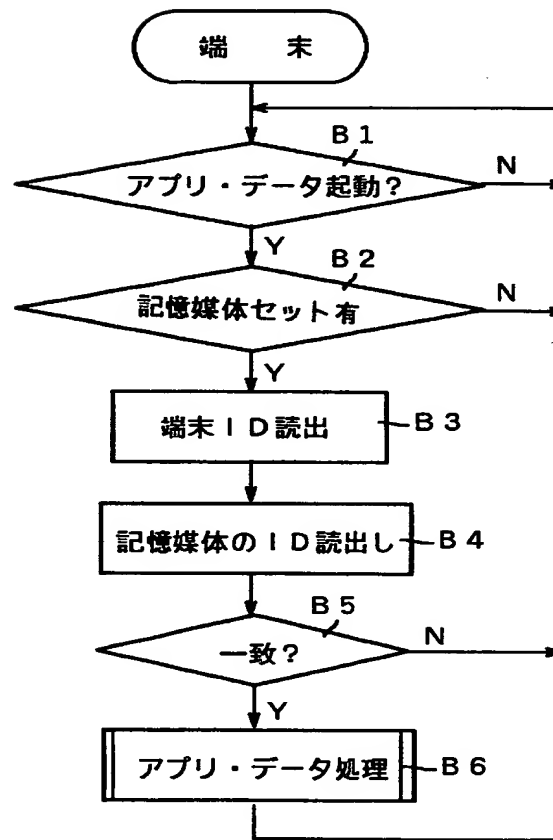
【图 5】



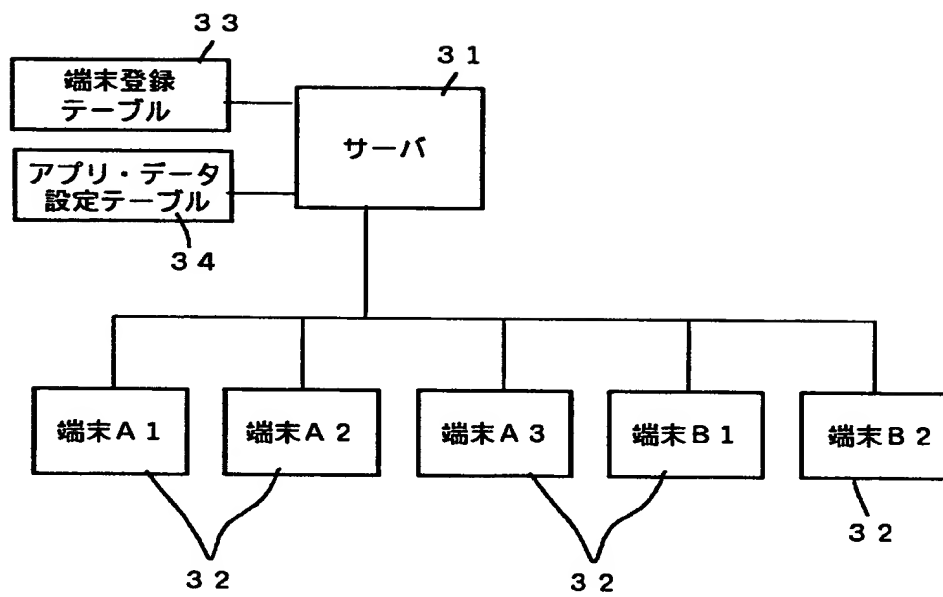
【図 6】



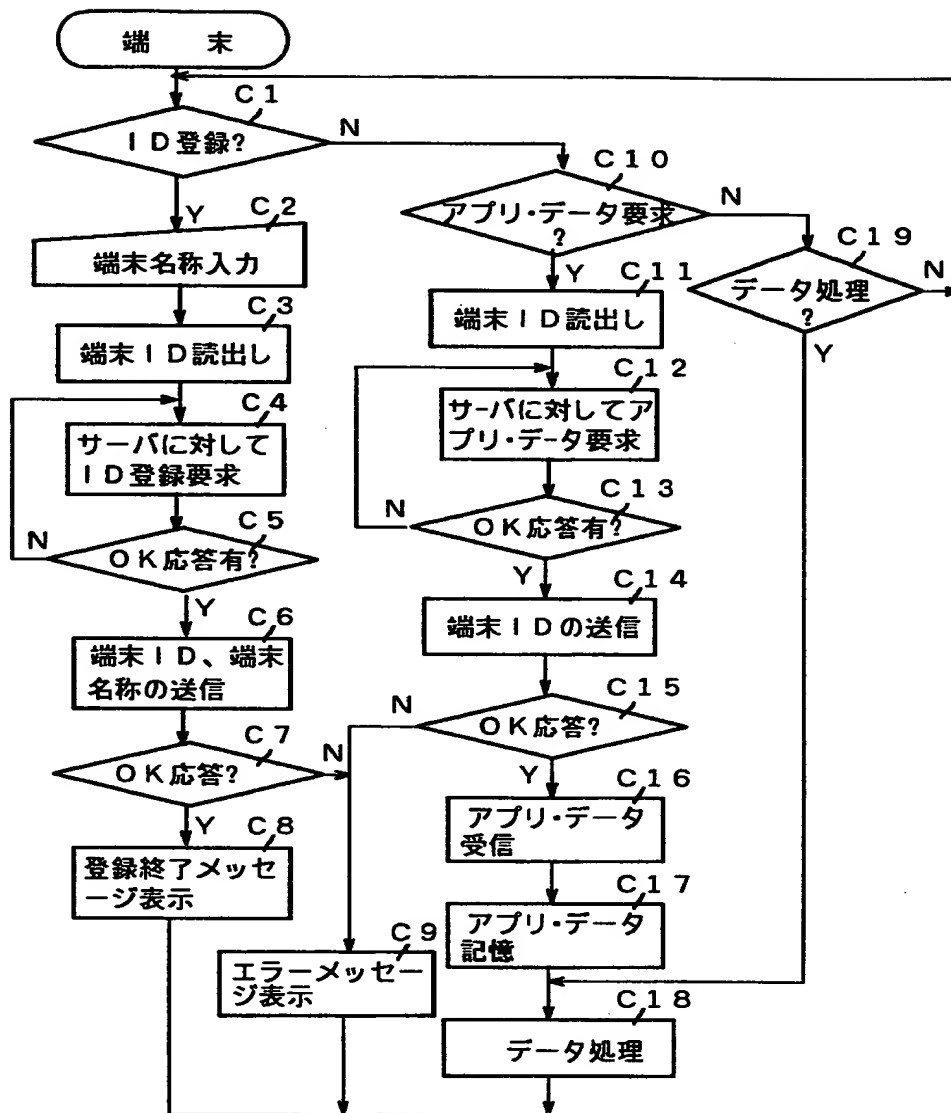
【図 7】



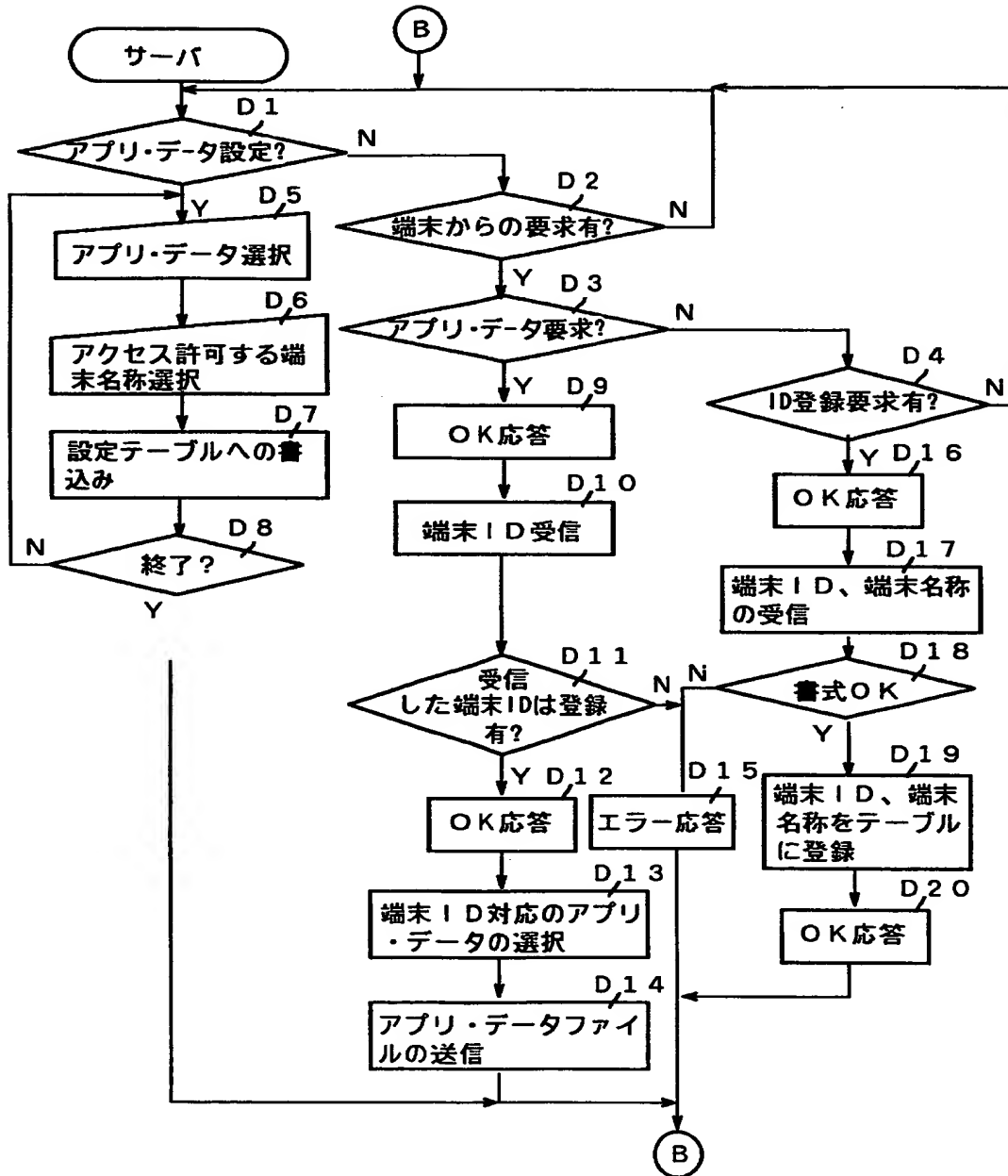
【図 8】



【図 9】



【図 1 0】



【書類名】 要約書

【要約】

【課題】 アプリケーションソフト／データが格納されている記録媒体をアクセスしてデータ処理を行うデータ処理装置において、特定のデータ処理装置に対してのみ記録媒体内のアプリケーションソフト／データのアクセスを許可することで、装置毎のアクセス制御が可能となり、セキュリティ維持と共にアクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止する。

【解決手段】 APソフト／データベースが格納されている持ち運び自在なCFカード3がセットされている状態で、このCFカード3内のAPソフト／データベースをアクセスしてデータ処理を行う携帯端末2において、携帯端末2はCFカード3内に予め格納されている端末IDを読み込む。そして、このCFカード3内の端末IDと予め設定されている自己の端末IDとを比較し、その比較結果に基づいてCFカード3内のAPソフト／データベースに対するアクセス可否を決定する。

【選択図】 図1

認定・付加情報

特許出願の番号	平成11年 特許願 第121200号
受付番号	59900410994
書類名	特許願
担当官	第七担当上席 0096
作成日	平成11年 6月 2日

<認定情報・付加情報>

【提出日】	平成11年 4月28日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000001443]

1. 変更年月日 1998年 1月 9日
[変更理由] 住所変更
住 所 東京都渋谷区本町1丁目6番2号
氏 名 カシオ計算機株式会社